UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,987	04/19/2004	Paul A. Gassoway	063170.7003	3477

5073   7590   10/02/2007

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER
ZEE, EDWARD

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
10/02/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

	Application No.	Applicant(s)
Office Action Summary	10/826,987	GASSOWAY, PAUL A.
	Examiner	Art Unit	
	Edward Zee	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _12 July 2007_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-26_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-26_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This is in response to the amendment filed on July 12th, 2007. Claims 1, 5, 9-11, 16, 20

and 24-26 have been amended and Claims 1-26 are pending and have been considered below.

Specification

2.   The amendments filed on July 12th, 2007 to the specification have been considered and

effectively overcome the previous objections. Therefore the previous objections to the

specification have been withdrawn.

Claim Objections

3.   The amendments filed on July 12th, 2007 to Claims 10, 15 and 24-26 have been

considered and effectively overcome the previous objections. Therefore the previous objections

to Claims 10, 15 and 24-26 have been withdrawn.

Claim Rejections - 35 USC § 101

4.   The amendments filed on July 12th, 2007 to Claim 16 has been considered and effectively

overcome the previous 35 USC § 101 rejections. Therefore the previous rejections have been

withdrawn. The Examiner notes that the Applicant has amended Claim 16 to disclose a

"**tangible** computer storage medium", which is not defined in the specification. Therefore, the

Examiner will interpret this storage medium as not encompassing any form of electronic

transmission signals.

Claim Rejections - 35 USC § 102

5.   The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

6.   **Claims 1-5, 9, 11 and 16-20 are rejected under 35 U.S.C. 102(b) as being anticipated**

by Ji et al. (5,623,600).

Claims 1 and 16: Ji et al. discloses a method and computer storage medium containing code for

maintaining computer security comprising:

        a. providing a signature file [column 7, lines 51-65]. The examiner notes that it is

inherent to provide a signature file when performing a signature scanning virus detection

method;

        b. receiving an incoming message from at least one client computer*(downloaded from*

the web) [column 5, lines 28-38];

        c. comparing the received incoming message with the signature file to determine whether

the incoming message is malicious*(performs a version of signature scanning virus detection)*

[column 7, lines 51-65];

        d. and blocking*(do not transfer file)* the incoming messages determined to be malicious

from reaching a web server [column 8, lines 4-16].

Claims 2-4 and 17-19: Ji et al. discloses a method and computer storage medium as in claims 1

and 16 above and further discloses that the comparing further comprises:

        a. parsing the incoming message*(scanning the message body)* [column 10, lines 26-28].

The examiner notes that scanning the message body implies parsing the message into at least a

message header and message body;

b. converting the incoming message into an internal format *(decoding encoded portions)* [column 10, lines 57-67];

c. comparing the converted incoming message with the signature file and determining whether the converted incoming message is malicious based on the comparison *(executes a virus-checking program)* [column 11, lines 1-2];

d. reassembling the converted incoming message back into its original format prior to forwarding *(transmits the message)* it to the web server if it is determined that the code is not malicious *(no viruses are detected)* and forwarding *(transmits the message)* the reassembled message to the web server [column 10, lines 42-56 and column 11, lines 4-6].

Claims 5 and 20: Ji et al. discloses a method as in claims 1 and 16 above and further discloses that the signature file contains information about known system vulnerabilities [column 7, lines 51-65]. The examiner notes that it is inherent for the signature file to contain information about vulnerabilities in order for the virus detection program to know what kind of vulnerabilities it is scanning for.

Claim 9: Ji et al. discloses a system for maintaining computer security comprising:

a. a signature file [column 7, lines 51-65]. The examiner notes that it is inherent to provide a signature file when performing a signature scanning virus detection method;

b. a web server *(gateway node)* [column 3, lines 52-63];

c. and a proxy machine *(proxy server)* receiving an incoming message from at least one client computer, comparing the received incoming message with the signature file to determine whether t he incoming message is malicious and blocking incoming messages determined to be malicious from reaching the web server [column 4, lines 56-67].

Claim 11: Ji et al. discloses a system as in claim 9 above and further discloses that the signature

file contains information about known system vulnerabilities [column 7, lines 51-65]. The

examiner notes that it is inherent for the signature file to contain information about

vulnerabilities in order for the virus detection program to know what kind of vulnerabilities it is

scanning for.

Claim Rejections - 35 USC § 103

7.   The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

8.   **Claims 6-8, 12-14 and 21-23 are rejected under 35 U.S.C. 103(a) as being**

unpatentable over Ji et al. (5,623,600) in view of Cambridge (7,080,000).

Claims 6, 12 and 21: Ji et al. discloses a method, system and computer storage medium as in

claims 1, 9 and 16 above, but does not explicitly disclose that the signature file is made available

through a web server. However, Cambridge discloses a similar method, system and computer

storage medium and further discloses that the signature file*(antivirus database)* is made available

through a web server*(antivirus server)* [abstract]. Therefore, it would have been obvious to one

of ordinary skill in the art at the time of invention to make the signature files available through a

web server. One would have been motivated to do so in order to make signature file updates

easily accessible.

Claims 7, 13 and 22: Ji et al. discloses a method, system and computer storage medium as in

claims 1, 9 and 16 above, but does not explicitly disclose continuously updating the signature

file. However, Cambridge discloses a similar method, system and computer storage medium and

further discloses continuously updating the signature file *(antivirus data file)* [column 2, lines 63-67]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to continuously update the signature file. One would have been motivated to do so in order to be able to detect the latest viruses, which are constantly being created.

Claims 8, 14 and 23: Ji et al. discloses a method, system and computer storage medium as in claims 1, 9 and 16 above, but does not explicitly disclose periodically downloading the signature file in order to make its copy current. However, Cambridge discloses a similar method, system and computer storage medium and further discloses periodically downloading the signature files *(receiving a new antivirus file at one of the user computers)* in order to make its copy current [abstract]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to periodically download the signature files. One would have been motivated to do so in order to be able to detect the latest viruses, which are constantly being created.

9.   **Claims 10, 15 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ji et al. (5,623,600).**

Claim 10: Ji et al. discloses a system as in claim 9 above and further discloses that the proxy machine further comprises:

        a. a message parser module for receiving, parsing *(scanning the message body)* and converting *(decoding encoded portions)* the incoming messages into a defined format [column 10, lines 26-28 and column 10, lines 57-67]. The examiner notes that scanning the message body implies parsing the message into at least a message header and message body.

        b. a message analyzer module for comparing the converted incoming messages with the signature file *(executes a virus-checking program)* [column 11, lines 1-2;

c. and a message reassembly module for reassembling the converted incoming messages

determined not to be malicious*(no viruses are detected)* into their original format and forwarding

them to the web server*(transmits the message)* [column 10, lines 42-56 and column 11, lines 4-

6].

However, Ji et al. does not explicitly disclose that the message parser, analyzer and reassembly

modules are HTTP message parser, analyzer and reassembly modules. Nonetheless, it would

have been obvious to one of ordinary skill in the art at the time of invention to employ an HTTP

message parser, analyzer and reassembly modules. One would have been motivated to do so in

order to capable of processing HTTP messages instead of other forms of electronic messages,

depending on the intended application of the system.

Claim 15: Ji et al. discloses a system as in claim 10 above and further discloses that the

signature file is linked to the HTTP message analyzer module*(executes a virus-checking

program)* [column 11, lines 1-2]. The examiner notes that it is inherent for the HTTP message

analyzer to be linked to the signature file if it is using the signature file to scan for viruses.

Claims 24-26: Ji et al. disclose a method, system and computer storage medium as in claims 1, 9

and 16 above, but does not explicitly disclose that the incoming message comprises an HTTP

messages. However, it would have been obvious to one of ordinary skill in the art at the time of

invention for the incoming messages to be comprised of HTTP messages. One would have been

motivated to do so in order to be capable of processing HTTP messages instead of other forms of

electronic messages, depending on the intended application of the system.

Response to Arguments

10.   Applicant's arguments filed on July 12th, 2007 have been fully considered but they are not

persuasive.

11.   Regarding independent Claims 1, 9 and 16 the Applicant argues that Ji et al. does not

disclose "comparing the received incoming message" with a "signature file containing

information about known system vulnerabilities" as required by Claims 1, 9 and 16.

       However, the Examiner respectfully disagrees and submits that Ji et al. does in fact

disclose comparing the message with a signature file *(ie. signature scanning)* [column 2, lines 1-

5]. The Applicant even suggests that Ji et al. is in fact performing this "signature scanning" and

appears to equate this to "searches for known patterns of program code used for viruses", [page

10, lines 11-14 of the amendments filed on July 12th, 2007]. Thus, the Examiner respectfully

submits that, searching for "known patterns of program code used for viruses" implies that one is

given at least a list of these "known patterns", which is usually packaged in a virus definitions

file(ie. signature file), before performing the searching(ie. comparison).

Conclusion

12.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

       A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing
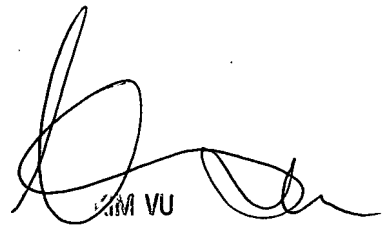
date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The

examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
September 26, 2007

KIM VU
PATENT EXAMINER
TECHNOLOGY CENTER 2100